Solution Brief

Banking/Financial Services, Health and Life Sciences, Defense/Government, Networking/Telco

Arqit and Intel Bring Post-Quantum Cryptography to Network Edge

Arqit's NetworkSecure is pre-packaged on platforms based on Intel® NetSec Accelerator Reference Design and delivers secure encryption key generation for edge AI, PQC and data sovereignty applications

The Problem We Solve

For cybersecurity and IT leaders, quantum computing is a present-day risk that requires organizations to start planning their journey to post-quantum migration today.

The current risk comes from adversaries preparing for that future moment when quantum computers become more widely available. Cyberthieves, nation-state operators, and organized crime groups are stealing and storing encrypted data today through harvest now, decrypt later (HNDL) attacks, with a strategy to decrypt and use that data once quantum computers mature. For organizations with confidentiality timelines of 10, 20, or up to 50 years, this represents a profound risk.

To understand the magnitude of the challenge, it's important to look at what quantum computing does to current encryption schemes. Most of today's public-key cryptography—such as RSA and elliptic-curve cryptography—is protected by the computational hardness of mathematical problems that are impractical for classical systems to crack at scale.

Quantum computers, however, will be able to use advanced algorithms such as Shor's algorithm to break these cryptographic technologies in hours or minutes. This means the core mechanisms that protect everything from bank transactions to medical records to national security systems will become vulnerable once sufficiently powerful quantum computers emerge.

One area of vulnerability is the network edge. Organizations are moving a significant portion of their compute capability to where data is created and consumed. Without new encryption technologies, these computers could be targets of HNDL attacks.

Post-Quantum Cryptography at the Edge: Solution Overview

The solution is a transition to post-quantum cryptography (PQC)—a new class of cryptographic algorithms designed to withstand attacks from both classical and quantum computers. Governments worldwide recognize both the urgency and the complexity of this shift. Many are requiring organizations to begin PQC migrations now in order to finalize the transition between 2030 and 2035.

At the same time, governments are publishing standards, frameworks, and transition guidance to help organizations understand which algorithms to adopt and how to deploy them. An example of this effort is the US National Security Agency's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), which specifies the quantum-resistant algorithms required for national security systems.

Even with these standards, transitioning to PQC – especially at the edge - within just a few years is a significant challenge. Enterprises must inventory their

cryptographic assets, upgrade infrastructure, ensure interoperability, and manage long deployment cycles.

The importance of network edge exchanging ever so valuable information also creates data sovereignty challenges as organizations look for solutions to guarantee the confidentiality, portability and availability of data stored across distributed environments. Many are starting to realize that residency alone isn't enough to satisfy regulators and their own resilience requirements.

Arqit, an Intel® Industry Solutions Builders Partner, offers an edge PQC solution that is designed to run on Intel® architecture processors to deliver an integrated and easy to install solution that extends PQC protection to the network edge. Together, Arqit and Intel address the challenges of data sovereignty through Arqit NetworkSecure™, which leverages Intel® Trust Domain Extensions (Intel® TDX) to enhance the confidentiality of both data in use and data in transit for sensitive workloads deployed across hosted environments.

Our Solution Components

Arqit NetworkSecure

Arqit NetworkSecure is a comprehensive suite of software comprised of the company's NetworkSecure-Controller (NS-Controller) that generates PQC encryption keys. In the Arqit NS-Controller, the controller function can be deployed both in the cloud and on-premises.

The option to deploy NS-Controller at the edge minimizes round trip delay for cloud access and pushes keys at very high speeds and with low latency, enabling key generation even where internet connection speeds are unstable or have limited bandwidth. The NS-Controller also provides full capability at the edge in air-gapped environments without any external internet connectivity. NetworkSecure can be delivered pre-packaged on Intel-based servers in PCIe add-in-card form factor (based on Intel® NetSec Accelerator Reference Design) to conveniently reduce the time-to-deployment of the solution.

In Figure 1, NetworkSecure endpoints (in gray) generate symmetric keys that are used by firewalls, routers or other data systems that handle encrypted traffic. For the NetworkSecure endpoints to generate encryption keys, they use a locally installed NS-Controller that can be situated in an onsite data center or other local compute center. All of the endpoints and the controller can run on servers in PCIe add-in-card based on Intel NetSec Accelerator Reference Design.

Intel® Xeon® SoC Powers Servers Based on Intel NetSec Accelerator Reference Design

Intel NetSec Accelerator Reference Design add-in-cards are designed to provide additional compute power or isolated server resources for applications running on the server system, including network infrastructure and security function processing, offloading the tasks from the host CPU. Since the Intel NetSec Accelerator Reference Design specifies Intel processors, it provides coherent computing architecture where the same Intel architecture optimized software can be executed on both the server host CPU and on the add-in-card.

The cards that Arqit delivers with NetworkSecure are powered by Intel® Xeon® D processors or Intel® Xeon® 6 SoC and feature up to dual 100G QSFP28 ports for high-speed optical network connectivity. The combination of this processor and high-speed networking delivers efficient compute and networking offload in a PCIe Gen5 x8 form factor.

To protect NetworkSecure at the edge, Arqit utilizes Intel TDX on the Intel Xeon 6 SoC. Intel TDX enables a hardware-based trusted execution environment (TEE) that facilitates the deployment of trust domains (TD), that are hardware-isolated and encrypted virtual machines (VM) designed to protect sensitive data and applications from unauthorized access including the host machine root administrator. The TEE hardens the NetworkSecure deployment and is especially useful for applications where data sovereignty is a requirement because users have an extra measure of control and security around their applications.

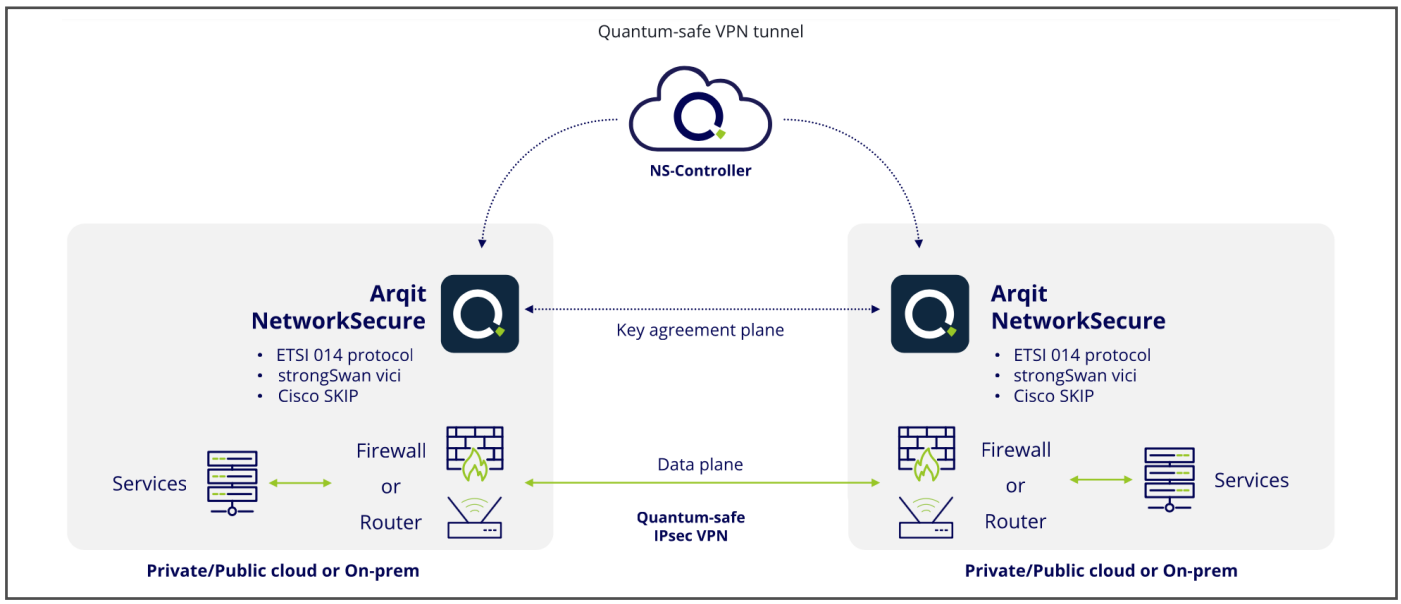

Figure 1. An example of the network configuration and data flows for Arqit NetworkSecure deployments.

Deployment Flexibility

NetworkSecure can be used in a variety of use cases in many industries, including:

Telco as a Service: NetworkSecure enables telcos and service providers to offer quantum-safe VPNs as a premium to Network as a Service (NaaS) model. NetworkSecure is scalable to thousands of endpoints — including mobile devices, uCPE and private 5G base stations. NetworkSecure offers protection for data in transit across untrusted networks. High availability and disaster recovery features support resilient network architectures and telco-grade SLAs.

Enterprise: NetworkSecure is ideal for branch offices, restaurants, hotels and even remote locations like oil rigs and offshore wind farms. As more of these locations process sensitive and higher value information from point-of-sale machines, IoT sensors, and office-based edge devices there is a growing need for this data to be protected as it's sent to centralized locations for further processing.

Military: Modern military operations require the ability to rapidly deploy mobile, scalable and agile command-and-control (C2) infrastructure in a range of diverse scenarios. Solutions must be efficient, with low OpEx/CapEx, and support a range of hardware, software and networks and deliver robust security today and in the future. NetworkSecure offers a highly secure and scalable option for agile C2, to ensure mission success with confidence. It delivers improved flexibility, assurance and maneuverability, with low overhead, a small form factor, and low power requirements.

Conclusion

Edge computing will remain a target of HNDL attacks if something is not done to deliver PQC to these sites. With more data being created at the edge, and the clock ticking on the availability of quantum computers, organizations need to act quickly to find a solution. Into this situation, Arqit has developed its NetworkSecure that is pre-packaged on PCIe add-in-card compute modules based on the Intel NetSec Accelerator Reference Design. The PCIe card format allows this solution to be easily installed into a network by inserting the card into an existing Intel architecture server for rapid and cost-efficient deployments. With local key generation and controller capabilities, NetworkSecure eliminates cloud dependency, providing high-throughput, low latency key generation. This enables the journey toward data sovereignty by ensuring that encryption keys are only visible to the devices that need them, and no other entity, government or third party.

Learn More

Arqit NetworkSecure

Arqit SKA Edge Controller

Intel® Xeon® D processor

Intel® Xeon® 6 SoC

Intel® Trust Domain Extensions (Intel® TDX)

Intel® Ethernet Controller E810

Intel® Ethernet Controller E830

Intel® NetSec Accelerator Reference Design

Intel® Industry Solutions Builders

Arqit and Intel - Accelerate the Journey to Data Sovereignty and Quantum-Safe Networks

intel.

0426/MK/DJA/PDF Please Recycle 368510-001EN